(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-352910
(P2005-352910A)
(43)公開日　平成17年12月22日(2005.12.22)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 15/00	G06F 15/00	330A	5B017
G06F 12/14	G06F 12/14	530C	5B085
	G06F 12/14	530E	

審査請求 有　請求項の数 7　OL　（全 24 頁）

(21)出願番号　特願2004-174630 (P2004-174630)
(22)出願日　平成16年6月11日 (2004.6.11)

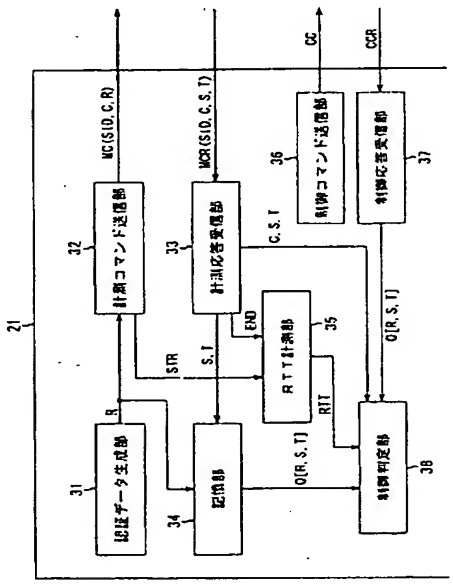
(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番３５号
(74)代理人　100082131
弁理士　稲本　義雄
(72)発明者　嶋　久登
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

Fターム(参考)　5B017 AA03　BB10　CA16
5B085 AE00

(54)【発明の名称】情報処理装置および方法

(57)【要約】
【課題】例えば著作権で保護されたコンテンツを適切に提供する。
【解決手段】計測コマンド送信部３２は、認証データRを含む計測コマンドMCを受信機器に送信する。計測応答受信部３３は、送信された計測コマンドMCに対する、受信機器からの応答MCRを受信する。記憶部３４は、計測コマンドMCの認証データR、および受信機器からの応答MCRの応答データSと応答生成時間Tを記憶する。RTT計測部３５は、往復伝播時間（RTT）を計測する。制御コマンド送信部３６は、制御コマンドCCを受信機器に送信する。制御応答受信部３７は、制御コマンドCCに対する受信側の機器からの応答CCRを受信する。制御判定部３８は、RTTに基づいて、受信機器が同じLAN１内にあるものか否かを判定するとともに、受信機器から正規の機器しか知り得ない情報の提供を受けて、受信機器へのコンテンツの送信を判定する。
【選択図】図４

図4



【特許請求の範囲】
【請求項１】
ネットワークに接続された受信装置に対する所定のコンテンツの送信可否を、所定のコマンドに対する応答にかかる応答時間に基づいて判定する情報処理装置において、
前記受信装置からの、前記コマンドに対する、所定の応答データを含む応答を受信する受信手段と、
前記受信装置からの、前記コマンドに対する応答時間を計測する計測手段と、
前記計測手段により計測された前記応答時間に基づいて、前記受信装置を認証する認証手段と、
前記コマンドに挿入される認証データを生成する生成手段と、
前記生成手段により生成された前記認証データの中の所定のものを含む前記コマンドを、前記認証手段による認証が成功するまで最大ｋ回、前記受信装置に送信する送信手段と、
前記送信手段により送信された前記コマンドに含まれる前記認証データと、前記受信手段により受信された前記応答に含まれる前記応答データを記憶する記憶手段と、
前記認証手段により認証された前記受信装置に対して、第ｎ番目に受信された前記コマンドに含まれていた認証データと、その前記コマンドに対する応答に含まれていた応答データの送信を要求する要求手段と、
前記要求手段による要求に応じて、前記受信装置から送信されてきた前記認証データおよび応答データと、第ｎ番目に送信したコマンドに含まれていた認証データおよびそのコマンドに対する応答に含まれていた応答データとが一致するか否かを判定し、その判定結果に基づいて、前記コンテンツの前記受信装置への送信可否を判定する判定手段と
を備えることを特徴とする情報処理装置。
【請求項２】
前記判定手段は、前記要求手段による要求に応じて、前記受信装置から送信されてきた、前記認証データ、前記応答データ、および前記コンテンツを利用できる装置間で共有する共有データから生成された署名に基づいて、前記受信装置を認証する
ことを特徴とする請求項１に記載の情報処理装置。
【請求項３】
前記計測手段は、前記送信手段により前記コマンドが送信されたときから、前記コマンドに対応する応答が前記受信手段により受信されるまでの時間を、前記応答時間として計測する
ことを特徴とする請求項１に記載の情報処理装置。
【請求項４】
ネットワークに接続された受信装置に対する所定のコンテンツの送信可否を、所定のコマンドに対する応答にかかる応答時間に基づいて判定する情報処理方法において、
前記受信装置からの、前記コマンドに対する、所定の応答データを含む応答を受信する受信ステップと、
前記受信装置からの、前記コマンドに対する応答時間を計測する計測ステップと、
前記計測ステップの処理で計測された前記応答時間に基づいて、前記受信装置を認証する認証ステップと、
前記コマンドに挿入される認証データを生成する生成ステップと、
前記生成ステップの処理で生成された前記認証データの中の所定のものを含む前記コマンドを、前記認証ステップの処理での認証が成功するまで最大ｋ回、前記受信装置に送信する送信ステップと、
前記送信ステップの処理で送信された前記コマンドに含まれる前記認証データと、前記受信ステップの処理で受信された前記応答に含まれる前記応答データを記憶する記憶ステップと、
前記認証ステップの処理で認証された前記受信装置に対して、第ｎ番目に受信された前記コマンドに含まれていた認証データと、その前記コマンドに対する応答に含まれていた

応答データの送信を要求する要求ステップと、
前記要求ステップの処理での要求に応じて、前記受信装置から送信されてきた前記認証データおよび応答データと、第ｎ番目に送信したコマンドに含まれていた認証データおよびそのコマンドに対する応答に含まれていた応答データとが一致するか否かを判定し、その判定結果に基づいて、前記コンテンツの前記受信装置への送信可否を判定する判定ステップと
を含むことを特徴とする情報処理方法。
【請求項５】
ネットワークに接続される送信装置から所定のコンテンツの提供を受ける情報処理装置において、前記送信装置から送信されてきた、所定の認証データを含むコマンドを受信する受信手段と、
前記コマンドに対する、所定の応答データを含む応答を、前記送信装置に送信する第１の送信手段と、
前記送信装置からの要求に応じて、第ｎ番目に受信されてきた前記コマンドに含まれている認証データと、その前記コマンドに対する応答に含まれていた応答データを、前記送信装置に送信する第２の送信手段と
を備えることを特徴とする情報処理装置。
【請求項６】
前記第２の送信手段は、前記認証データ、前記応答データ、および前記コンテンツを利用できる装置間で共有する共有データに基づいて署名を生成して、前記送信装置に送信することを特徴とする請求項５に記載の情報処理装置。
【請求項７】
ネットワークに接続される送信装置から所定のコンテンツの提供を受けるための情報処理方法において、
前記送信装置から送信されてきた、所定の認証データを含むコマンドを受信する受信ステップと、
前記コマンドに対する、所定の応答データを含む応答を、前記送信装置に送信する第１の送信ステップと、
前記送信装置からの要求に応じて、第ｎ番目に受信されてきた前記コマンドに含まれている認証データと、その前記コマンドに対する応答に含まれていた応答データを、前記送信装置に送信する第２の送信ステップと
を含むことを特徴とする情報処理方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置および方法に関し、特に、例えば著作権で保護されたコンテンツを適切に授受することができるようにした情報処理装置および方法に関する。
【背景技術】
【０００２】
近年、インターネットに代表される公共性のある広域に亘るネットワーク（以下、WAN(Wide Area Network)と称する）や一般家屋等に設けられる局所的なネットワーク（以下、LAN(Local Area Network)と称する）の普及に伴い、それらのネットワークを介した各種データ通信が盛んに行われている。
【０００３】
映像や音楽コンテンツなどを、ネットワークを通して伝送する場合は、著作権保護のために、通信相手の機器との間で、認証および鍵交換を行い、コンテンツを暗号化して伝送することが行われている（非特許文献１参照）。
【０００４】
ここにおいて、著作権の観点からは、家庭内でのコピーや伝送は許可するが、WANで接続された他の家庭との間でのコンテンツの伝送を制限したい場合がある。例えば、テレビ

ジョン放送を録画したコンテンツは、私的利用の範囲（家庭内）で利用できるが、インターネットを通して、他人に伝送するのは著作権を侵害すると考えられるので、このような制限が必要となる。

【０００５】

この制限の下では、著作権保護されたコンテンツを送信する機器(送信機器)は、そのコンテンツを受信する通信相手の機器(受信機器)が同一LAN内にあるか、WAN(インターネット)を通して接続されているかを判断する必要がある。

【０００６】

例えば、IPアドレスから通信相手が同一サブネット内にあるかどうかを調べることや、IP通信パケットが通過したIPルータの数(Hop Count)を使うことで通信相手がWAN(インターネット)を通して接続されているかを知ることができる。しかしながら、WAN(インターネット)を経由した通信であってもVPN(Virtual Private Network)などの技術を使えば、IPルータを経由せずに接続されている同一サブネットであるかように接続することが可能である。すなわち不正にコンテンツを入手することが可能である。

【０００７】

そこで、通信相手との間の通信の往復伝播時間(RTT: Round Trip Time)を計測することによって通信距離を判別する方法が提案されている。これはインターネットなどのWANでは、通信距離が長いことおよび、途中のルーターなどの処理にかかる時間などのために、通信データの伝播にかかる時間が家庭内のLANに比べて長くなることを利用するものである。

【０００８】

例えば図１Ａに示すように、送信機器において、受信機器への計測コマンド（Ｓ１）の伝送時間、受信機器からの計測コマンドに対する応答（Ｓ２）の伝送時間等の往復伝播時間を計測する。同一家庭内のネットワークにおける往復伝播時間は、所定の規定時間（例えば5mS）かそれ以下であるのに比べ、この例のように、インターネット（WAN）を経由した通信は、それ以上（例えば7mS）かかるので、往復伝播時間の長短によって、受信機器がWANを通じて接続されていることを判別することができる。

【０００９】

【非特許文献１】DTCP Specification Volume 1 Version 1.3 (Information Version) http://www.dtcp.com/daTa/info_20040107_dtcp_Vol_1_1p3.pdf

【発明の開示】

【発明が解決しようとする課題】

【００１０】

しかしながら例えば、往復伝播時間だけで、コンテンツの送信可否を判定すると、図１Ｂに示すように、途中に（例えば同一LANに）第３の機器ｘを挿入して、計測コマンドに応答することによって、往復伝播時間を短縮することができ、コンテンツを不正に入手することができる。

【００１１】

そこで受信機器しか知りえない情報をもって応答させることもできるが、図１Ｃのように機器ｘがあらかじめ受信機器に計測コマンド（Ｓ２１）を送って、受信機器しか知り得ない情報に基づく応答（Ｓ２２）を取得しておき、送信機器から計測コマンド（Ｓ３１）が来たときに、覚えておいた応答を返すようにようにすれば（Ｓ３２）、正規の機器になりすますことができる。

【００１２】

本発明は、このような状況に鑑みてなされたものであり、例えば著作権で保護されたコンテンツを適切に授受することができるようにするものである。

【課題を解決するための手段】

【００１３】

本発明の第１の情報処理装置は、受信装置からの、コマンドに対する、所定の応答データを含む応答を受信する受信手段と、受信装置からの、コマンドに対する応答時間を計測

する計測手段と、計測手段により計測された応答時間に基づいて、受信装置を認証する認証手段と、コマンドに挿入される認証データを生成する生成手段と、生成手段により生成された認証データの中の所定のものを含むコマンドを、認証手段による認証が成功するまで最大ｋ回、受信装置に送信する送信手段と、送信手段により送信されたコマンドに含まれる認証データと、受信手段により受信された応答に含まれる応答データを記憶する記憶手段と、認証手段により認証された受信装置に対して、第ｎ番目に受信されたコマンドに含まれていた認証データと、そのコマンドに対する応答に含まれていた応答データの送信を要求する要求手段と、要求手段による要求に応じて、受信装置から送信されてきた認証データおよび応答データと、第ｎ番目に送信したコマンドに含まれていた認証データおよびそのコマンドに対する応答に含まれていた応答データとが一致するか否かを判定し、その判定結果に基づいて、コンテンツの受信装置への送信可否を判定する判定手段とを備えることを特徴とする。

【００１４】

判定手段は、要求手段による要求に応じて、受信装置から送信されてきた、認証データ、応答データ、およびコンテンツを利用できる装置間で共有する共有データから生成された署名に基づいて、受信装置を認証することができる。

【００１５】

計測手段は、送信手段によりコマンドが送信されたときから、コマンドに対応する応答が受信手段により受信されるまでの時間を、応答時間として計測することができる。

【００１６】

本発明の第１の情報処理方法は、受信装置からの、コマンドに対する、所定の応答データを含む応答を受信する受信ステップと、受信装置からの、コマンドに対する応答時間を計測する計測ステップと、計測ステップの処理で計測された応答時間に基づいて、受信装置を認証する認証ステップと、コマンドに挿入される認証データを生成する生成ステップと、生成ステップの処理で生成された認証データの中の所定のものを含むコマンドを、認証ステップの処理での認証が成功するまで最大ｋ回、受信装置に送信する送信ステップと、送信ステップの処理で送信されたコマンドに含まれる認証データと、受信ステップの処理で受信された応答に含まれる応答データを記憶する記憶ステップと、認証ステップの処理で認証された受信装置に対して、第ｎ番目に受信されたコマンドに含まれていた認証データと、そのコマンドに対する応答に含まれていた応答データの送信を要求する要求ステップと、要求ステップの処理での要求に応じて、受信装置から送信されてきた認証データおよび応答データと、第ｎ番目に送信したコマンドに含まれていた認証データおよびそのコマンドに対する応答に含まれていた応答データとが一致するか否かを判定し、その判定結果に基づいて、コンテンツの受信装置への送信可否を判定する判定ステップとを含むことを特徴とする。

【００１７】

本発明の第１の情報処理装置および方法においては、受信装置からの、コマンドに対する、所定の応答データを含む応答が受信され、受信装置からの、コマンドに対する応答時間が計測され、計測された応答時間に基づいて、受信装置が認証され、コマンドに挿入される認証データが生成され、生成された認証データの中の所定のものを含むコマンドが、認証が成功するまで最大ｋ回、受信装置に送信され、送信されたコマンドに含まれる認証データと、受信ステップの処理で受信された応答に含まれる応答データが記憶され、認証された受信装置に対して、第ｎ番目に受信されたコマンドに含まれていた認証データと、そのコマンドに対する応答に含まれていた応答データの送信が要求され、要求に応じて、受信装置から送信されてきた認証データおよび応答データと、第ｎ番目に送信したコマンドに含まれていた認証データおよびそのコマンドに対する応答に含まれていた応答データとが一致するか否かが判定され、その判定結果に基づいて、コンテンツの受信装置への送信可否が判定される。

【００１８】

本発明の第２の情報処理装置は、送信装置から送信されてきた、所定の認証データを含

むコマンドを受信する受信手段と、コマンドに対する、所定の応答データを含む応答を、送信装置に送信する第１の送信手段と、送信装置からの要求に応じて、第ｎ番目に受信されてきたコマンドに含まれている認証データと、そのコマンドに対する応答に含まれていた応答データを、送信装置に送信する第２の送信手段とを備えることを特徴とする。

【００１９】

第２の送信手段は、認証データ、応答データ、およびコンテンツを利用できる装置間で共有する共有データに基づいて署名を生成して、送信装置に送信することができる。

【００２０】

本発明の第２の情報処理方法は、送信装置から送信されてきた、所定の認証データを含むコマンドを受信する受信ステップと、コマンドに対する、所定の応答データを含む応答を、送信装置に送信する第１の送信ステップと、送信装置からの要求に応じて、第ｎ番目に受信されてきたコマンドに含まれている認証データと、そのコマンドに対する応答に含まれていた応答データを、送信装置に送信する第２の送信ステップとを含むことを特徴とする。

【００２１】

本発明の第２の情報処理装置および方法においては、送信装置から送信されてきた、所定の認証データを含むコマンドが受信され、コマンドに対する、所定の応答データを含む応答が、送信装置に送信され、送信装置からの要求に応じて、第ｎ番目に受信されてきたコマンドに含まれている認証データと、そのコマンドに対する応答に含まれていた応答データが、送信装置に送信される。

【発明の効果】

【００２２】

本発明によれば、例えば著作権で保護されたコンテンツを適切に授受することができる。

【発明を実施するための最良の形態】

【００２３】

以下に本発明の実施の形態を説明するが、本明細書に記載の発明と、発明の実施の形態との対応関係を例示すると、次のようになる。この記載は、本明細書に記載されている発明をサポートする実施の形態が本明細書に記載されていることを確認するためのものである。従って、発明の実施の形態中には記載されているが、発明に対応するものとして、ここには記載されていない実施の形態があったとしても、そのことは、その実施の形態が、その発明に対応するものではないことを意味するものではない。逆に、実施の形態が発明に対応するものとしてここに記載されていたとしても、そのことは、その実施の形態が、その発明以外の発明には対応しないものであることを意味するものでもない。

【００２４】

さらに、この記載は、本明細書に記載されている発明の全てを意味するものではない。換言すれば、この記載は、本明細書に記載されている発明であって、この出願では請求されていない発明の存在、すなわち、将来、分割出願されたり、補正により出現、追加される発明の存在を否定するものではない。

【００２５】

本発明の第１の情報処理装置は、受信装置からの、コマンドに対する、所定の応答データを含む応答を受信する受信手段（例えば、図４の計測応答受信部３３）と、受信装置からの、コマンドに対する応答時間を計測する計測手段（例えば、図４のRTT計測部３５）と、計測手段により計測された応答時間に基づいて、受信装置を認証する認証手段（例えば、図４の制御判定部３８）と、コマンドに挿入される認証データを生成する生成手段（例えば、図４の認証データ生成部３１）と、生成手段により生成された認証データの中の所定のものを含むコマンドを、認証手段による認証が成功するまで最大ｋ回、受信装置に送信する送信手段（例えば、図４の計測コマンド送信部３２）と、送信手段により送信されたコマンドに含まれる認証データと、受信手段により受信された応答に含まれる応答データを記憶する記憶手段（例えば、図４の記憶部３４）と、認証手段により認証された受

信装置に対して、第ｎ番目に受信されたコマンドに含まれていた認証データと、そのコマンドに対する応答に含まれていた応答データの送信を要求する要求手段（例えば、図４の制御コマンド送信部３６）と、要求手段による要求に応じて、受信装置から送信されてきた認証データおよび応答データと、第ｎ番目に送信したコマンドに含まれていた認証データおよびそのコマンドに対する応答に含まれていた応答データとが一致するか否かを判定し、その判定結果に基づいて、コンテンツの受信装置への送信可否を判定する判定手段（例えば、図４の制御判定部３８）とを備えることを特徴とする。

【００２６】

本発明の第１の情報処理方法は、受信装置からの、コマンドに対する、所定の応答データを含む応答を受信する受信ステップ（例えば、図６のステップＳ５６）と、受信装置からの、コマンドに対する応答時間を計測する計測ステップ（例えば、図６のステップＳ５５，Ｓ５９）と、計測ステップの処理で計測された応答時間に基づいて、受信装置を認証する認証ステップ（例えば、図６のステップＳ６１）と、コマンドに挿入される認証データを生成する生成ステップ（例えば、図６のステップＳ５３）と、生成ステップの処理で生成された認証データの中の所定のものを含むコマンドを、認証ステップの処理での認証が成功するまで最大ｋ回、受信装置に送信する送信ステップ（例えば、図６のステップＳ５４乃至ステップＳ６３）と、送信ステップの処理で送信されたコマンドに含まれる認証データと、受信ステップの処理で受信された応答に含まれる応答データを記憶する記憶ステップ（例えば、図６のステップＳ５５，Ｓ６０）と、認証ステップの処理で認証された受信装置に対して、第ｎ番目に受信されたコマンドに含まれていた認証データと、そのコマンドに対する応答に含まれていた応答データの送信を要求する要求ステップ（例えば、図６のステップＳ６４）と、要求ステップの処理での要求に応じて、受信装置から送信されてきた認証データおよび応答データと、第ｎ番目に送信したコマンドに含まれていた認証データおよびそのコマンドに対する応答に含まれていた応答データとが一致するか否かを判定し、その判定結果に基づいて、コンテンツの受信装置への送信可否を判定する判定ステップ（例えば、図６のステップＳ６６）とを含むことを特徴とする。

【００２７】

本発明の第２の情報処理装置は、送信装置から送信されてきた、所定の認証データを含むコマンドを受信する受信手段（例えば、図５の計測コマンド受信部５３）と、コマンドに対する、所定の応答データを含む応答を、送信装置に送信する第１の送信手段（例えば、図５の計測応答送信部５５）と、送信装置からの要求に応じて、第ｎ番目に受信されてきたコマンドに含まれている認証データと、そのコマンドに対する応答に含まれていた応答データを、送信装置に送信する第２の送信手段（例えば、図５の制御応答送信部５８）とを備えることを特徴とする。

【００２８】

本発明の第２の情報処理方法は、送信装置から送信されてきた、所定の認証データを含むコマンドを受信する受信ステップ（例えば、図７のステップＳ８６）と、コマンドに対する、所定の応答データを含む応答を、送信装置に送信する第１の送信ステップ（例えば、図７のステップＳ９２）と、送信装置からの要求に応じて、第ｎ番目に受信されてきたコマンドに含まれている認証データと、そのコマンドに対する応答に含まれていた応答データを、送信装置に送信する第２の送信ステップ（例えば、図７のステップＳ９４）とを含むことを特徴とする。

【００２９】

図２は、本発明を適用した端末１１からなる通信システムの構成例を示している。

【００３０】

ＬＡＮ１－１，１－２（以下、個々に区別する必要がない場合、単に、ＬＡＮ１と称する。他の場合についても同様である）がインターネットに代表されるＷＡＮ２を介して相互に接続されている。

【００３１】

ＬＡＮ１－１は、例えば、家屋内に設けられ、特定の個人（あるいは、家族）が使用する

程度の規模のものであり、それには、スイッチングハブ（図示せず）を介して、パーソナルコンピュータやＡＶ機器等の端末１１－１および端末１１－２が接続されている。LAN１－１と端末１１－１および１１－２との接続は、例えば、Ethernet(登録商標)（100BASE-TX）等の高速インタフェースによって行われる。端末１１－１および１１－２は、LAN１－１およびWAN２を介して、LAN１－２に接続することができる。

【００３２】

LAN１－２は、LAN１－１と同様に構成されており、それには、端末１１－３が接続されている。

【００３３】

各端末１１は、著作権で保護される所定のコンテンツを授受できる機器として登録された機器（以下、適宜、このような機器を、正規の機器と称する）である。各端末１１は、同一LAN１内ある他の端末１１と、このコンテンツを授受することができる。

【００３４】

端末１１は、図３に示すように、送信可否判定部２１、応答制御部２２、通信部２３、およびコンテンツ格納部２４を含んで構成されている。

【００３５】

送信可否判定部２１は、著作権で保護されたコンテンツ（例えばコンテンツ格納部２４に格納されているコンテンツ）を送信する際、受信側の機器との往復伝播時間(RTT: Round Trip Time)に基づいて、受信側の機器が同じLAN１内にあるものか否かを判定するとともに、受信側の機器から正規の機器しか知り得ない情報の提供を受けて、RTT計測の相手と正規の機器しか知り得ない情報の提供者が同一であるか否かを確認する。送信可否判定部２１は、この確認結果に基づいて、コンテンツの送信の可否を判定する。

【００３６】

図１Ｃの例では、RTT計測の相手（機器ｘ）と、正規の機器か知り得ない情報の提供者（受信機器）との同一性を確認しなかったので、送信機器と同一LANに挿入された不正な機器ｘは、受信機器から、正規の機器しか知り得ない情報を送信機器に供給させることによって、送信機器からコンテンツを不正に入手することができた。しかしながら本発明によれば、後述するようにRTT計測の相手（機器ｘ）と、正規の機器しか知り得ない情報の提供者（受信機器）が同一であることが確認されるので、図１Ｃに示したような不正は排除される。

【００３７】

応答制御部２２は、送信側の端末１１から所定のコンテンツの提供を受ける際、通信部２３を介して、送信側の機器と後述するように通信することで、コンテンツの提供を受けるために必要な情報（RTT計測に必要なデータ、正規の機器しか知り得ない情報、およびRTT計測の相手と正規の機器しか知り得ない情報の提供者が同一であることを確かめるための情報）を送信側の機器に送信する。

【００３８】

通信部２３は、LAN１に接続されており、同一のLAN１内の機器、またはWAN２を介して異なるLAN１に接続されている機器との通信を行う。

【００３９】

コンテンツ格納部２４は、受信側の端末１１に送信されるコンテンツが格納されている。このコンテンツは、例えば著作権で保護されており、その著作権によりその利用が許可された端末１１であって、送信側の端末１１と同一LAN１に接続された端末１１にのみ提供される。

【００４０】

図４は、端末１１の送信可否判定部２１の構成例を示している。

【００４１】

認証データ生成部３１は、RTT計測のために受信側の機器に送信される計測コマンドMCを構成する認証データRを生成する。この認証データRは、ランダムチャレンジとして使用されるので、疑似乱数列などの、毎回異なる予測不可能な数列で構成されている。

【００４２】
計測コマンド送信部３２は、認証データ生成部３１で生成された認証データRを含む計測コマンドMCを、受信側の機器に送信する。
【００４３】
計測応答受信部３３は、計測コマンド送信部３２により送信された計測コマンドMCに対する、受信側の機器からの応答MCRを受信する。
【００４４】
記憶部３４は、計測コマンドMCに挿入された認証データR、および計測コマンドMCに対する受信側の機器からの応答MCRに含まれている応答データSと応答生成時間T（後述）を記憶する。
【００４５】
RTT計測部３５は、計測コマンド送信部３２および計測応答受信部３３からの通知STR, ENDに応じて、受信側の機器との通信往復伝播時間（RTT）を計測する。
【００４６】
制御コマンド送信部３６は、開始コマンドや確認コマンド（後述）の制御コマンドCCを受信側の機器に送信する。制御応答受信部３７は、制御コマンドCCに対する受信側の機器からの応答CCRを受信する。
【００４７】
制御判定部３８は、上記各部を制御し、受信側の機器との往復伝播時間(RTT)に基づいて、受信側の機器が同じLAN１内にあるものか否かを判定するとともに、受信側の機器から正規の機器しか知り得ない情報の提供を受けて、RTT計測の相手と正規の機器しか知り得ない情報の提供者が同一であるか否かを確認する。制御判定部３８は、この確認結果に基づいて、コンテンツの送信可否を判定する。
【００４８】
なお図４の各部を結ぶ矢印は、主なデータの送受信の流れを表している。
【００４９】
図５は、端末１１の応答制御部２２の構成例を示している。
【００５０】
応答データ生成部５２は、計測コマンドMCに対する応答MCRを構成する応答データSを生成する。この応答データSは、ランダムチャレンジとして使用されるので、疑似乱数列など、毎回異なる予測不可能な数列で構成されている。なおここで生成された応答データSと、送信側の機器で生成される認証データRは、それぞれ独立して生成されており、両者が共有するものではない。
【００５１】
計測コマンド受信部５３は、送信側の機器からの計測コマンドMCを受信する。
【００５２】
応答生成時間計測部５４は、計測コマンド受信部５３からの通知STR, ENDに応じて、計測コマンドMCに対する応答MCRを生成するのに要した時間（以下、応答生成時間と称する）Tを計測する。
【００５３】
計測応答送信部５５は、RTT計測に必要なデータ（応答データSおよび応答生成時間T（後述）等）を含む、計測コマンドMCに対する応答MCRを生成し、送信側の機器に送信する。
【００５４】
記憶部５６は、計測コマンドMCに含まれていた認証データR、および応答MCRに含まれて送信された応答データSと応答生成時間Tを記憶する。
【００５５】
制御コマンド受信部５７は、送信側の機器から送信されてきた制御コマンドCCを受信する。制御応答送信部５８は、制御コマンドCCに対する応答CCRを送信側の機器に送信する。例えばRTT計測の相手と正規の機器しか知り得ない情報の提供者が同一であることを確

認するためのデータが、制御コマンドCCの応答CCRとして送信側の機器に送信される。

【００５６】

制御部５１は、上記各手段を制御する。

【００５７】

次に、送信可否判定処理（端末１１の送信可否判定部２１の処理）を、図６のフローチャートを参照して説明する。

【００５８】

ステップＳ５１において、端末１１の送信可否判定部２１の制御コマンド送信部３６は、受信側の機器と、TCPコネクションを確立する。TCPコネクションのためのポート番号は予め送信側の端末１１と受信側の機器の間で合意されているものとする。送信側の機器と受信側の機器の間で事前にTCPコネクションが確立している場合はこのステップを省略してよい。

【００５９】

制御コマンド送信部３６は、確立したTCPコネクションを介して、RTTの計測を開始する旨を表す開始コマンド（制御コマンドCC）を受信側の機器に送信する。この開始コマンドCCには、セッション番号SID、および送信側の端末１１が実行可能な、１セッションでのRTTのリトライ数（計測回数）ksが含まれている。

【００６０】

セッション番号SIDは、これから行われる受信側の機器に対する一連の認証処理（１つのセッション）に割り当てられた番号であり、この番号を送信側と受信側とで共有することにより、セッション毎に認証処理を区別することができる。

【００６１】

またRTT計測のために必要なデータ（例えば、計測コマンドMCやその応答MCR）の通信は、パケットの再送を行わないUDPでなされるので、通信状態によっては、データが途中で消滅してしまうなど、RTT計測が適切に行われない場合も考えられる。またネットワーク内の他の通信の影響を受けて、パケットの伝送に遅延が生じることもある。そこでRTT計測を何回かリトライ（再施行）できるようになされている。このリトライの回数は、送信側の機器と受信側の機器の設定によって異なることもあるので、この例ではここで送信側の機器のリトライ数（例えば、最大のリトライ数）ｋｓが受信側の機器に通知される。

【００６２】

次に、ステップＳ５２において、制御応答受信部３７は、開始コマンドCCに対する、受信側の機器からの応答CCRを受信する。

【００６３】

この応答CCRには、開始コマンドCCに含まれていたセッション番号SIDの他、受信側が決定した１セッションでのRTT計測のリトライ数k、および計測コマンドMCを受信するためのUDPポート番号ｐｂが含まれている。すなわち開始コマンドCCとその応答CCRにより、送信側の端末１１と受信側の機器は、RTT計測のリトライ数（計測回数）kとセッション番号SID、および計測コマンドMCとその応答MCRで利用するUDPポート番号ｐｂを合意する。

【００６４】

なお受信側の機器は、開始コマンドCCを介して通知された送信側の端末１１で実行可能なRTT計測のリトライ数ksと受信側が実行可能のRTT計測のリトライ数のうちの小さい方を、RTT計測のリトライ数kに決定し、応答CCRを介して送信側の機器に通知する。

【００６５】

ステップＳ５３において、認証データ生成部３１は、ステップＳ５２で受信された応答CCRに含まれていたRTT計測のリトライ数k分の認証データ（k個の認証データ）Ｒを生成する。

【００６６】

ステップＳ５４において、制御判定部３８に内蔵されるカウンタiの値が１に初期設定される。このとき認証データ生成部３１は、カウンタiの値に対応する認証データ（例えば、第ｉ番目に生成された認証データRi）を、計測コマンド送信部３２および記憶部３４

に供給する。

【００６７】

ステップＳ５５において、計測コマンド送信部３２は、セッション番号SID、認証データ生成部３１から供給された認証データRi（k個の認証データRのうちのカウンタiの値に対応する認証データRi）、およびシーケンス番号Ci（カウンタiの値を表す番号）を含む計測コマンドMCを、制御コマンドCCの応答CCRに含まれていたUDPポート番号ｐｂでのUDP通信で、受信側の機器に送信する。

【００６８】

計測コマンド送信部３２は、計測コマンドMCを送信したとき、その旨の通知STRをRTT計測部３５に行う。これによりRTT計測部３５は、RTTの計測を開始する。

【００６９】

記憶部３４は、認証データ生成部３１から供給された認証データRiを、カウンタiの値に対応させて（シーケンス番号Ciに対応させて）記憶する。

【００７０】

ステップＳ５６において、計測応答受信部３３は、受信側の機器からの応答MCRを受信したか否かを判定し、受信していないと判定した場合、ステップＳ５７に進み、所定時間以上応答を待っているか否かを判定する（ステップＳ５５でRTT計測が開始されてから所定の時間経過したか否かを判定する）。

【００７１】

ステップＳ５７で、まだ所定の時間していないと判定された場合、ステップＳ５６に戻り、それ以降の処理が実行される。一方ステップＳ５７で所定の時間経過したと判定された場合、ステップＳ６２に進み、カウンタiの値がリトライ数kより大きいか否かが判定され（RTT計測がk回行われたか否かが判定され）、まだ大きくないと判定された場合（k回行われていない場合）、ステップＳ６３に進み、カウンタiの値を１だけインクリメントされて、ステップＳ５５に戻る。

【００７２】

計測コマンドMCを送るUDPでは、パケットが通信相手に届かないことがあるので、送信側の端末１１は、計測コマンドMCを送った後、所定時間が経っても応答MCRが受信されない場合は、この回の計測は失敗したものとして、次のRTT計測が開始される（ステップＳ５５に戻る）。

【００７３】

ステップＳ５６で、応答MCRが受信されたと判定された場合、ステップＳ５８に進み、計測応答受信部３３は、受信した応答MCRに含まれている応答データSj、シーケンス番号Cj、および応答生成時間Tjを読み出し、制御判定部３８に供給する。

【００７４】

制御判定部３８は、計測応答受信部３３から供給されたシーケンス番号Cjが、カウンタiの値（送信された計測コマンドMCのシーケンス番号Ci）と一致するか否かを判定する。なお応答MCRのシーケンス番号Cjと計測コマンドMCのシーケンス番号Ciを確認する意味については後述する。

【００７５】

ステップＳ５８において、一致しないと判定された場合、ステップＳ５６に戻り、それ以降の処理が行われ、一致すると判定された場合、ステップＳ５９に進む。

【００７６】

ステップＳ５９において、計測応答受信部３３は、応答MCRを受信した旨の通知ENDをRTT計測部３５に行う。RTT計測部３５は、ステップＳ５５で開始したRTT計測を終了し、計測結果（RTT）を、制御判定部３８に供給する。

【００７７】

ステップＳ６０において、計測応答受信部３３は、受信した応答MCRに含まれていた応答データSjおよび応答生成時間Tjを、記憶部３４に供給する。記憶部３４は、カウンタiの値に対応させて、計測応答受信部３３から供給された応答データSjと応答生成時間Tjを

記憶する。すなわち記憶部３４には、カウンタiの値に対応して、認証データRi（ステップＳ５５）、応答データSj、および応答生成時間Tjが記憶される。

【００７８】

なお応答生成時間Tとは、詳細は後述するが、受信側の機器で、計測コマンドMCに対する応答MCRを生成するのに要した時間である。

【００７９】

ステップＳ６１において、制御判定部３８は、RTT計測部３５から供給されたRTTから、計測応答受信部３３から供給された応答生成時間Tj（応答MCRに含まれていた応答生成時間Tj）を減算し、その減算結果得られた値が、所定の規定時間ＴＬより大きいか否かを判定する。

【００８０】

ここで計測されたRTTは、計測コマンドMCの受信側の機器への伝送時間、受信側での応答MCRを生成するのに要した応答生成時間T、そして応答MCRの送信側の端末１１への伝送時間の合計となるので、そこから応答MCRを生成するのに要した応答生成時間Tを減算することで、実質的な往復伝播時間を求めることができる。

【００８１】

規定時間ＴＬは、実質的な往復伝播時間が、送信側の端末１１と受信側の機器が同一LAN1に接続されていたならば、それを超えないであろう時間である。すなわち実質的な往復伝播時間が規定時間ＴＬより大きければ、受信側の機器は送信側の端末１１と同一のLAN1に接続されていないと判定することができる。一方、実質的な往復伝播時間が規定時間ＴＬより大きくない（それ以下である場合）、受信側の機器は送信側の端末１１と同一LAN1に接続されていると判定することができる。

【００８２】

ステップＳ６１で、YESの判定がなされたとき（第ｉ回目のRTT計測で、受信側の機器が送信側の端末１１と同一のLAN1に接続されているものではないと判定されたとき）、ステップＳ６２に進み、制御判定部３８は、カウンタiの値がkより大きい値か否か（RTT計測がk回リトライされたか否か）を判定し、大きくないと判定した場合（RTT計測がまだk回行われていない場合）、ステップＳ６３に進み、カウンタiの値が１だけインクリメントされる。このとき認証データ生成部３１は、カウンタiの新たな値に対応する認証データRiを、計測コマンド送信部３２および記憶部３４に供給する。

【００８３】

その後ステップＳ５５に戻り、それ以降の処理が行われる。すなわち実質的な往復伝播時間が規定時間ＴＬ内になる応答MCRが得られないときは、最大k回、RTT計測が行われる。

【００８４】

ステップＳ６１で、NOの判定がなされたとき（実質的な往復伝播時間が規定時間ＴＬ以下となる応答MCRが得られたとき）、ステップＳ６４に進む。

【００８５】

ステップＳ６４において、制御コマンド送信部３６は、このセッションで最後に受信した計測コマンドMCに含まれていた認証データRと、その計測コマンドMCに対する応答MCRに含まれていた応答データSと応答生成時間Tの送信を要求する制御コマンド（確認コマンド）CCを、受信側の機器に送信する。

【００８６】

ステップＳ６５において、制御応答受信部３７は、受信側の機器から送信されてきた、ステップＳ６４で送信された確認コマンドCCに対する応答CCRを受信すると、それを制御判定部３８に供給する。

【００８７】

応答CCRには、例えば受信側の機器が最後に受信した計測コマンドMCに含まれている認証データRと、その計測コマンドMCに対する応答MCRに含まれていた応答データSと応答生成時間Tに対して、正規の機器が共有する秘密鍵に基づくハッシュ処理が施されたハッシュ値（署名）が示されている。

【００８８】
ステップＳ６６において、制御判定部３８は、制御応答受信部３７から供給された応答CCRに基づいて、受信側の機器にコンテンツを送信できるか否かを判定する。
【００８９】
具体的には制御判定部３８は、最後に受信側の機器に送信した計測コマンドMCに含まれていた認証データRと、その計測コマンドMCに対する応答MCRに含まれていた応答データSと応答生成時間Tを記憶部３４から読み出すとともに、正規の機器が共有する秘密鍵に基づくハッシュ処理を施す。
【００９０】
そして制御判定部３８は、応答CCRに示されるハッシュ値と、ここでのハッシュ処理の結果得られたハッシュ値が一致するか否かを判定し、一致すると判定した場合、RTT計測相手と、正規の機器のみが知り得る情報（署名）の提供者とが一致すると判定し、コンテンツを受信側の機器に送信できると判定する。RTT計測相手と正規の機器のみが知り得る情報の提供者とが一致することを確認するための認証データR、応答データS、および応答処理時間Tを、適宜、確認データQと称する。
【００９１】
また応答CCRに示される署名が、確認データQの全部または一部が著作権保護のための秘密鍵で暗号化されて生成されている場合、制御判定部３８は、その公開鍵でその署名を復号し、その結果得られた確認データQと、記憶部３４から読み出した確認データQが一致するか否かを判定する。
【００９２】
ステップＳ６６で、コンテンツを受信側の機器（端末１１）に送信できると判定された場合（RTT計測の相手と、正規の機器しか知り得ない情報の提供者が一致した場合）、ステップＳ６７に進み、制御判定部３８は、受信側の機器は、コンテンツを送信できる機器（コンテンツを利用できる機器であって、送信側の端末１１と同じLAN1に接続されている機器）である旨を、通信部２３（図３）に通知する。これにより通信部２３は、所定のコンテンツをコンテンツ格納部２４から読み出して、受信側の機器（端末１１）に送信する。
【００９３】
ステップＳ６６で、コンテンツを受信側の機器に送信できないと判定された場合（RTT計測の相手であった相手と、正規の機器しか知り得ない情報の提供者が一致しない場合）、ステップＳ６８に進み、制御判定部３８は、受信側の機器は、不正な機器であるとして、コンテンツを送信することができない旨を、通信部２３に通知する。これにより通信部２３は、コンテンツの受信側の機器への送信を行わない。
【００９４】
ステップＳ６２で、カウンタiの値が、kより大きいと判定された場合（RTT計測をk回行っても、実質的な往復伝播時間が規定時間TL以下になる応答MCRが得られなかった場合）、ステップＳ６９に進み、制御判定部３８は、受信側の機器は、ローカルネットワーク外の機器（同じLAN1に接続されていない機器）である旨を、通信部２４に通知する。これにより通信部２３は、コンテンツの受信側の機器への送信を行わない。
【００９５】
ステップＳ７０において、制御コマンド送信部３６は、終了コマンド（制御コマンド）CCを受信側の機器に送信する。
【００９６】
以上のようにして送信可否判定処理が行われる。
【００９７】
以上の説明では、ステップＳ５２においてk個の認証データRを生成したが、それに代えて、ステップＳ５５において、計測コマンドMCを送信する毎にそのコマンドに使う認証データRを毎回生成するようにしてもよい。
【００９８】

次に、応答制御処理（端末１１の応答制御部２２の処理）を、図７のフローチャートを参照して説明する。

【００９９】

ステップＳ８１において、端末１１の応答制御部２２の制御コマンド受信部５７は、送信側の機器と協働して、TCPコネクションを確立し、そのTCPコネクションを介して送信側の機器から送信されてきた、RTT計測の開始する旨を表す開始コマンドCC（ステップＳ５１）を受信する。

【０１００】

次にステップＳ８２において、計測コマンド受信部５３は、送信側の機器から送信されてくる計測コマンドMCを受信するためのUDPポート番号ｐｂを決定する。

【０１０１】

計測コマンド受信部５３はまた、制御コマンドCCに含まれている送信側の機器が実行可能なRTTのリトライ数ksと、受信側の端末１１が対応可能なRTT計測のリトライ数のいずれか小さい方を、今回のRTT計測のリトライ数kに決定する。そして応答データ生成部５２は、k個の応答データSを生成する。

【０１０２】

ステップＳ８３において、制御応答送信部５８は、ステップＳ８１で受信された制御コマンドCCに含まれていたセッション番号SID、RTT計測のリトライ数k、およびUDPポート番号ｐｂを含む応答CCRを、ステップＳ８１で確立されたTCPコネクトを介して送信側の機器に送信する。送信側の機器は、ここで送信された応答CCRを受信する（ステップＳ５２）。

【０１０３】

ステップＳ８４において、制御部５１に内蔵されているカウンタjの値が０に初期設定される。

【０１０４】

ステップＳ８５において、コマンドが受信されたか否かが判定され、コマンドが受信されたと判定された場合、ステップＳ８６に進み、受信されたコマンドが計測コマンドMC（ステップＳ５５）であるか否かを判定し、計測コマンドMCであると判定された場合、ステップＳ８７に進む。

【０１０５】

ステップＳ８７において、計測コマンド受信部５３は、計測コマンドMCに含まれているシーケンス番号Ciがカウンタjの値より大きいか否かを判定し、シーケンス番号Ciがカウンタjの値より大きいと判定した場合、ステップＳ８８に進む。なおここでの処理の意味については、図６のステップＳ５８の処理を合わせて後述する。

【０１０６】

ステップＳ８８において、計測コマンド受信部５３は、計測コマンドMCが受信された旨の通知STRを応答生成時間計測部５４に行う。これにより応答生成時間計測部５４は、応答生成時間の計測を開始する。

【０１０７】

ステップＳ８９において、カウンタjの値が計測コマンドMCに含まれているシーケンス番号Ciの値に設定される。このとき応答データ生成部５２は、設定されたカウンタjの値に対する応答データSjを、計測応答送信部５５および記憶部５６に供給する。

【０１０８】

次にステップＳ９０において、計測コマンド受信部５３は、受信した計測コマンドMCに含まれている認証データRiを読み出し、記憶部５６および計測応答送信部５５に供給する。記憶部５６は、計測コマンド受信部５３から供給された認証データRiを、カウンタjの値に対応させて記憶する。

【０１０９】

ステップＳ９１において、計測コマンド受信部５３は、認証データRiの読み出しが完了した旨の通知ENDを応答生成時間計測部５４に行う。これにより応答生成時間計測部５５

は、ステップＳ８８で開始した応答生成時間計測を終了し、計測結果Ｔｊを計測応答送信部５５および記憶部５６に供給する。

【０１１０】

ステップＳ９２において、計測応答送信部５５は、セッション番号SID、カウンタjの値を表すシーケンス番号Cj、応答データ生成部５２から供給された応答データSj、および応答生成時間計測部５４から供給された応答生成時間Tjを含む応答MCRを、送信側の機器に送信する。記憶部５６は、応答データSjおよび応答生成時間Tjを、カウンタjの値に対応させて記憶する。すなわち記憶部５６には、認証データRi（ステップＳ９０）、応答データSjおよび応答生成時間Tjが、カウンタjの値に対応して記憶されている。

【０１１１】

ステップＳ８６で、計測コマンドMCではないと判定された場合、ステップＳ９３に進み、確認コマンドCC（Ｓ６４）が受信されたか否かが判定され、確認コマンドCCが受信されたと判定した場合、ステップＳ９４に進む。

【０１１２】

ステップＳ９４において、制御応答送信部５８は、記憶部５６から、最後に受信された計測コマンドMCに含まれていた認証データRi、その計測コマンドMCに対する応答MCRに含まれていた応答データSjと応答生成時間Tjを、署名を付して、送信側の機器に送信する。

【０１１３】

ステップＳ９３で、確認コマンドCCではないと判定された場合（終了コマンドCC（ステップＳ７０）が受信された場合）、処理は終了する。

【０１１４】

以上のようにして、応答制御処理が実行される。

【０１１５】

以上の説明では、ステップＳ８２において最初にk個の応答データSを生成したが、それに代えて、ステップＳ９０において、計測コマンドMCを受信する毎にそのコマンドに対する応答MCRで使う応答データSを生成するようにしてもよい。あるいは、ステップＳ８２においては最初に１個の応答データS1を生成し、ステップＳ９２において応答MCRを送信した後に、次のコマンドMCに対する応答MCRの応答データSを生成するようにしてもよい。

【０１１６】

次に図６のステップＳ５８の処理の意味について説明する。ステップＳ５８の処理では、受信側の機器からの応答MCRのシーケンス番号Cjと計測コマンドMCのシーケンス番号Ci（カウンタiの値）が一致するか否かが判定されるが、このように計測コマンドMCと応答MCRの対応関係を確認するようにしたので、計測コマンドMCに対応しない応答MCR（他の計測コマンドMCの応答MCR）に基づいてRTT認証が行われないようにすることができる。

【０１１７】

例えば、図８に示すように、受信側の機器で、第１番目の計測コマンドMCに対する応答MCRの送信に時間がかかり（ステップＳ９２）、送信側の端末１１で、タイムアウトと判定されて（ステップＳ５７）、第２番目の計測コマンドMCが受信側の機器に送信されたものとする。第１番目の計測コマンドMCに対する応答MCRは、第２番目の計測コマンドMCが送信された後（ステップＳ５５）、第２番目の計測コマンドMCとの関係ではタイムアウトとならない間（ステップＳ５７）に送信側の端末１１に受信されたものとする（ステップＳ５６）。

【０１１８】

しかしながら本発明では、受信側の機器からの応答MCRのシーケンス番号（＝１）と、第２番目の計測コマンドMCのシーケンス番号（＝２）が一致しないと判定され、送信側の端末１１は、第２番目の計測コマンドMCに対する応答MCRが受信されるまで待機することになり（ステップＳ５６に戻る）、対応しない応答MCRが受信されてもRTT認証は行われない。

【０１１９】

次に図７のステップＳ８７の処理の意味を説明する。例えば図９に示すように、第１番

目の計測コマンドMCでのRTT計測で、規則時間TL内の応答MCRが得られず、第２番目の計測コマンドMCが送信される場合において、第２番目の計測コマンドMCの受信側の端末１１への到着が遅れ、第２番目の計測コマンドMCについてもタイムアウトと判定されて、送信側の機器からは第３番目の計測コマンドMCが受信側の端末１１へ送信されたとする。

【０１２０】

第２番目の計測コマンドMCは、第３番目の計測コマンドMCの受信の後、そしてその計測コマンドMCに対する応答MCRの送信の後、受信側の端末１１に到着したものとする。

【０１２１】

受信側の端末１１では、第２番目の計測コマンドMCの応答MCRを生成するとき、カウンタjの値は３になっているので（すでに第３番目の計測コマンドMCの応答MCRを生成しているので）、第２番目の計測コマンドMCに対する応答MCRを生成する際、第２番目の計測コマンドMCのシーケンス番号（＝２）＜カウンタj（＝３）であることからステップＳ８７でNOの判定がなされ、第２番目の計測コマンドMCに対する応答MCRは生成されない。

【０１２２】

すなわちステップＳ８７の処理により、計測コマンドMCに対応しない応答MCRに基づいてRTTの認証が行われないようになされている。

【０１２３】

次に、不正に対する端末１１の動作を具体的に説明する。

【０１２４】

例えば図１Ｃに示した、送信側の端末１１と同一のLAN１に接続された不正な機器ｘに対して、送信可否判定処理が開始されると、ステップＳ５１乃至ステップＳ５５の処理で、送信側の端末１１からは、図１０に示すように、第１番目の計測コマンドMCが不正機器ｘに送信される。

【０１２５】

不正機器ｘからは、応答制御処理におけるステップＳ８１乃至Ｓ９２の処理により、第１番目の計測コマンドMCの応答MCRが送信側の端末１１に送信される。

【０１２６】

この例の場合、不正機器ｘは、送信側の端末１１と同一のLAN１に接続されているので、RTT計測の結果、同一LAN１に接続されている機器と判定され（ステップＳ６１でNOの判定がなされ）、ステップＳ６４，Ｓ６５の処理により、送信側の端末１１から不正機器ｘへ確認コマンドCCが送信される。

【０１２７】

不正機器ｘは、第１番目の計測コマンドMCの応答MCRを送信した後、確認コマンドCCを受信すると、ステップＳ９４の処理により、最後の計測コマンドMCに含まれた認証データ（第１番目の計測コマンドMCの認証データR１）、その計測コマンドMCの応答MCRに含まれていた応答データS１と応答生成時間T１を送信側の端末１１に送信しようとする。しかしながら、不正機器ｘは、適切な署名を生成する情報を有していないので、例えば署名なしで若しくは不適当な署名を付してこれらのデータを応答CCRとして送信側の端末１１に送信する。

【０１２８】

送信側の端末１１はこの場合、署名の照合をすることができないので、RTT計測相手と正規の機器のみが知りうる情報の提供者が一致しないと判定し（ステップＳ６６）、コンテンツの送信は行われない（ステップＳ６８）。

【０１２９】

また計測コマンドMCに対する応答MCRは、送信側の端末１１と同じLAN１に接続されている不正機器ｘが行い、確認コマンドCCに対する応答CCRは正規の端末１１によって行われるようにする不正も考えられる。

【０１３０】

この場合不正機器ｘは、はじめに送信側の端末１１になりすまし、ステップＳ５１乃至ステップＳ５５の処理で、認証データRaを含む計測コマンドMCを受信側の端末１１に送信

し、受信側の端末１１から、ステップＳ８１乃至ステップＳ９２の処理で、応答データSaと応答生成時間Taを含む応答MCRを送信させて取得する。

【０１３１】

そしてその後は、不正機器ｘは、受信側の端末１１になりすまし、送信側の端末１１によるステップＳ５１乃至ステップＳ５５の処理により、送信側の端末１１から送信されてきた、認証データRbを含む計測コマンドMCを受信すると、先に正規の受信側の端末１１から取得しておいた応答MCRに含まれる応答データSaと、ステップＳ６１でNOの判定されるのに十分大きな応答生成時間Ta'を含む応答MCRを送信側の端末１１に送信する（ステップＳ９２）。

【０１３２】

その結果送信側の端末１１からは確認コマンドCCが送信されてくるので（ステップＳ６４）、不正機器ｘはそれをそのまま受信側の端末１１に送信する。確認コマンドCCを受信した受信側の端末１１は、最後に受信した計測コマンドMCに含まれる認証データ（いまの例の場合、不正機器ｘからの計測コマンドMCに含まれていた認証データRa）と、その計測コマンドMCに対する応答MCRに含まれていた応答データSaと応答生成時間Taに署名を付して、応答CCRとして送信側の端末１１に送信する。

【０１３３】

送信側の端末１１では、受信側の端末１１からの応答CCRの署名を解読することはできるが、この応答CCRに含まれる認証データRaが、送信側の端末１１が最後に送信した認証データ（不正機器ｘに送信した計測コマンドMCの認証データRb）と一致しないので（ステップＳ６６でNOの判定がなされるので）、不正機器ｘへのコンテンツ提供を行われない。

【０１３４】

このようにして本発明によれば、不正を適切に排除することができる。

【０１３５】

なお以上においては、受信側の端末１１において、応答生成時間を、応答MCRを生成する毎に計測したが、例えば最低必要な時間などの所定の時間に予め決めておき、その時間（固定値）を応答生成時間Tとすることもできる。

【０１３６】

また応答生成時間Tが通信往復伝播時間の計測に影響がないほどの大きさである場合（通信伝播時間が長い場合または受信側の機器の実装において、応答生成処理が十分に短い時間で行われる場合）は、応答生成時間Tを考慮する必要はない。

【図面の簡単な説明】

【０１３７】

【図１】従来の通信システムの利用例を示す図である。

【図２】本発明を適用した通信システムの利用例を示す図である。

【図３】図２の端末の構成例を示すブロック図である。

【図４】図３の送信可否判定部の構成例を示すブロック図である。

【図５】図３の応答制御部の構成例を示すブロック図である。

【図６】送信可否判定処理を説明するフローチャートである。

【図７】応答制御処理を説明するフローチャートである。

【図８】図２の端末の動作を説明する図である。

【図９】図２の端末の動作を説明する他の図である。

【図１０】図２の端末の動作を説明する他の図である。

【図１１】図２の端末の動作を説明する他の図である。

【符号の説明】

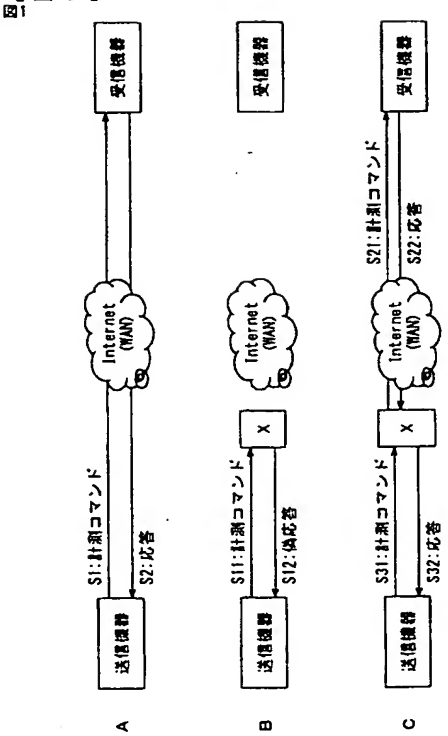
【０１３８】

１１　端末，　２１　送信可否判定部，　２２　応答制御部，　２３　通信部，　２４　コンテンツ格納部，　３１　認証データ生成部，　３２　計測コマンド送信部，　３３　計測応答受信部，　３４　記憶部，　３５　RTT計測部，　３６　制御コマンド送信部，　３７　制御応答受信部，　３８　制御判定部，　５１　制御部，　５２　応答データ

生成部，　５３　計測コマンド受信部，　５４　応答生成時間計測部，　５５　計測応答送信部，　５６　記憶部，　５７　制御コマンド受信部，　５８　制御応答送信部

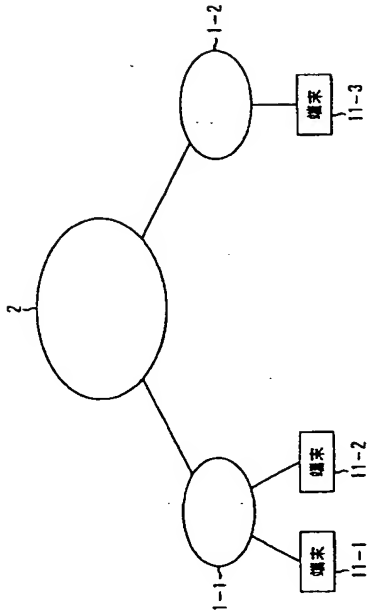
【図１】

図1

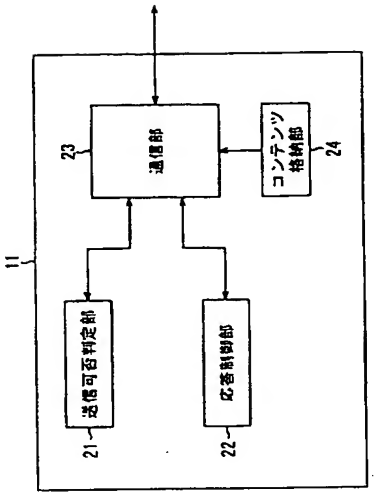


【図２】

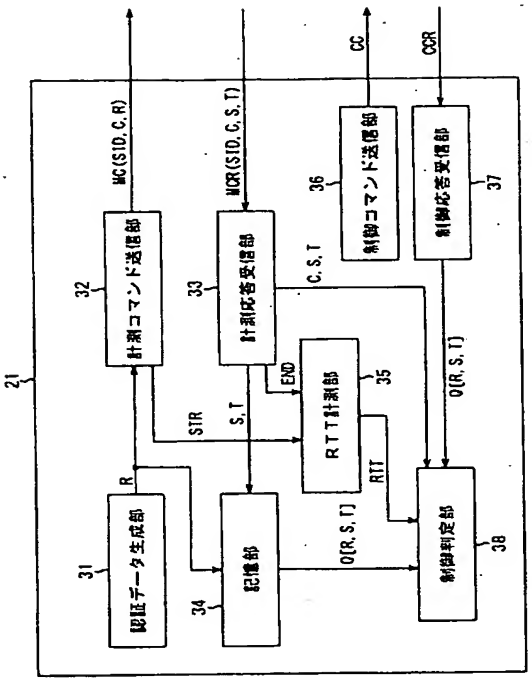
図2



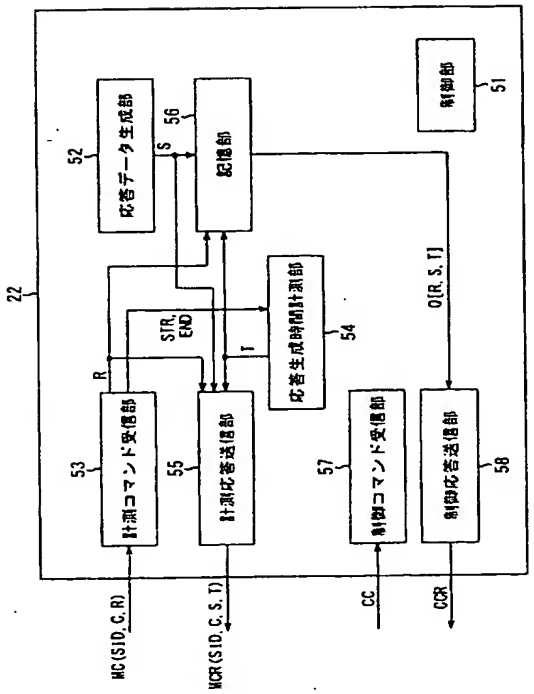
【図３】
図3



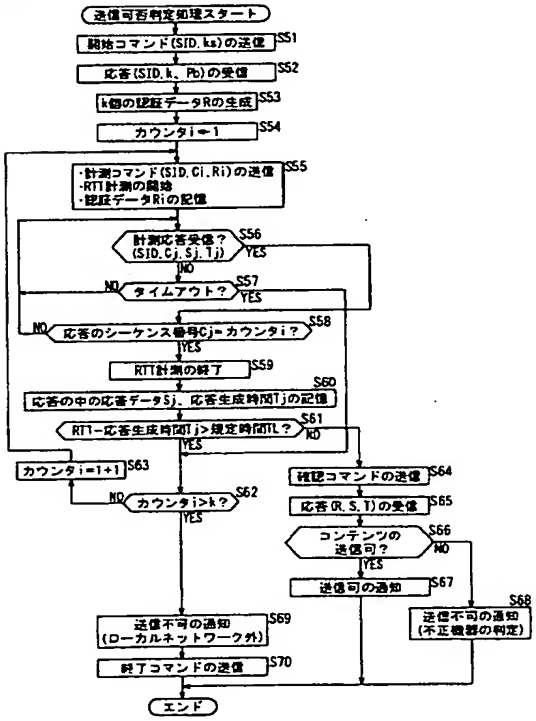
【図４】
図4



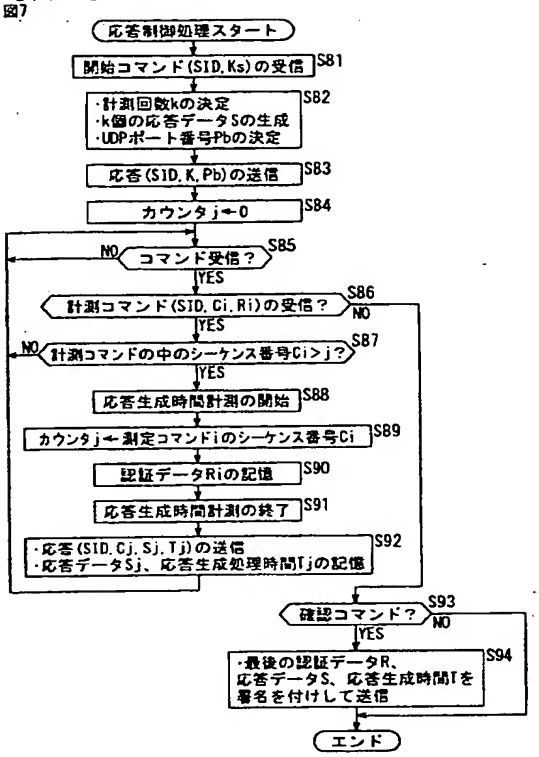
【図５】
図5



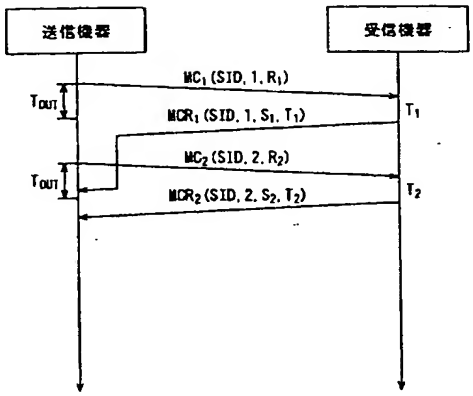
【図６】
図6



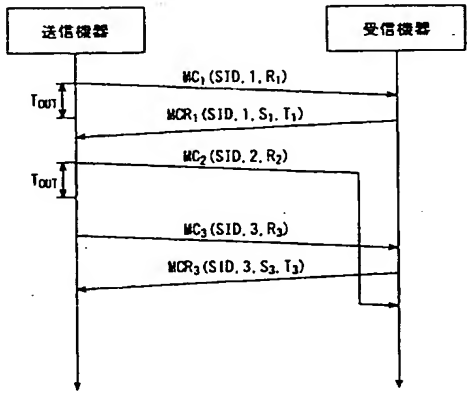
【図７】
図7



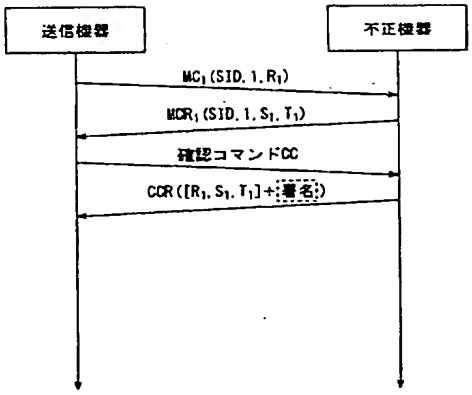
【図８】
図8



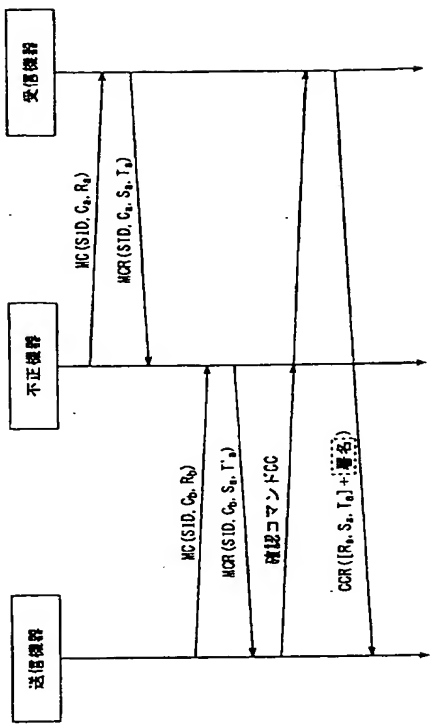
【図９】
図9



【図１０】
図10



【図１１】
図11



【手続補正書】
【提出日】平成17年7月15日(2005.7.15)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】００４２
【補正方法】変更
【補正の内容】
【００４２】
計測コマンド送信部３２は、認証データ生成部３１で生成された認証データRを含む計測コマンドMCを、受信側の機器にUDP通信で送信する。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００４６
【補正方法】変更
【補正の内容】
【００４６】
制御コマンド送信部３６は、開始コマンドや確認コマンド（後述）の制御コマンドCCを受信側の機器にTCP通信で送信する。制御応答受信部３７は、制御コマンドCCに対する受信側の機器からの応答CCRを受信する。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００５３
【補正方法】変更
【補正の内容】
【００５３】

計測応答送信部５５は、RTT計測に必要なデータ（応答データSおよび応答生成時間T（後述）等）を含む、計測コマンドMCに対する応答MCRを生成し、送信側の機器にUDP通信で送信する。

【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００５５
【補正方法】変更
【補正の内容】
【００５５】
制御コマンド受信部５７は、送信側の機器から送信されてきた制御コマンドCCを受信する。制御応答送信部５８は、制御コマンドCCに対する応答CCRを送信側の機器にTCP通信で送信する。例えばRTT計測の相手と正規の機器しか知り得ない情報の提供者が同一であることを確認するためのデータが、制御コマンドCCの応答CCRとして送信側の機器に送信される。

【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００５８
【補正方法】変更
【補正の内容】
【００５８】
まず始めに、端末１１の送信可否判定部２１の制御コマンド送信部３６は、受信側の機器と、TCPコネクションを確立する。TCPコネクションのためのポート番号は予め送信側の端末１１と受信側の機器の間で合意されているものとする。送信側の機器と受信側の機器の間で事前にTCPコネクションが確立している場合はこのステップを省略してよい。

【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００５９
【補正方法】変更
【補正の内容】
【００５９】
次に、ステップＳ５１において、制御コマンド送信部３６は、確立したTCPコネクションを介して、RTTの計測を開始する旨を表す開始コマンド（制御コマンドCC）を受信側の機器に送信する。この開始コマンドCCには、セッション番号SID、および送信側の端末１１が実行可能な、１セッションでのRTTのリトライ数（計測回数）ksが含まれている。

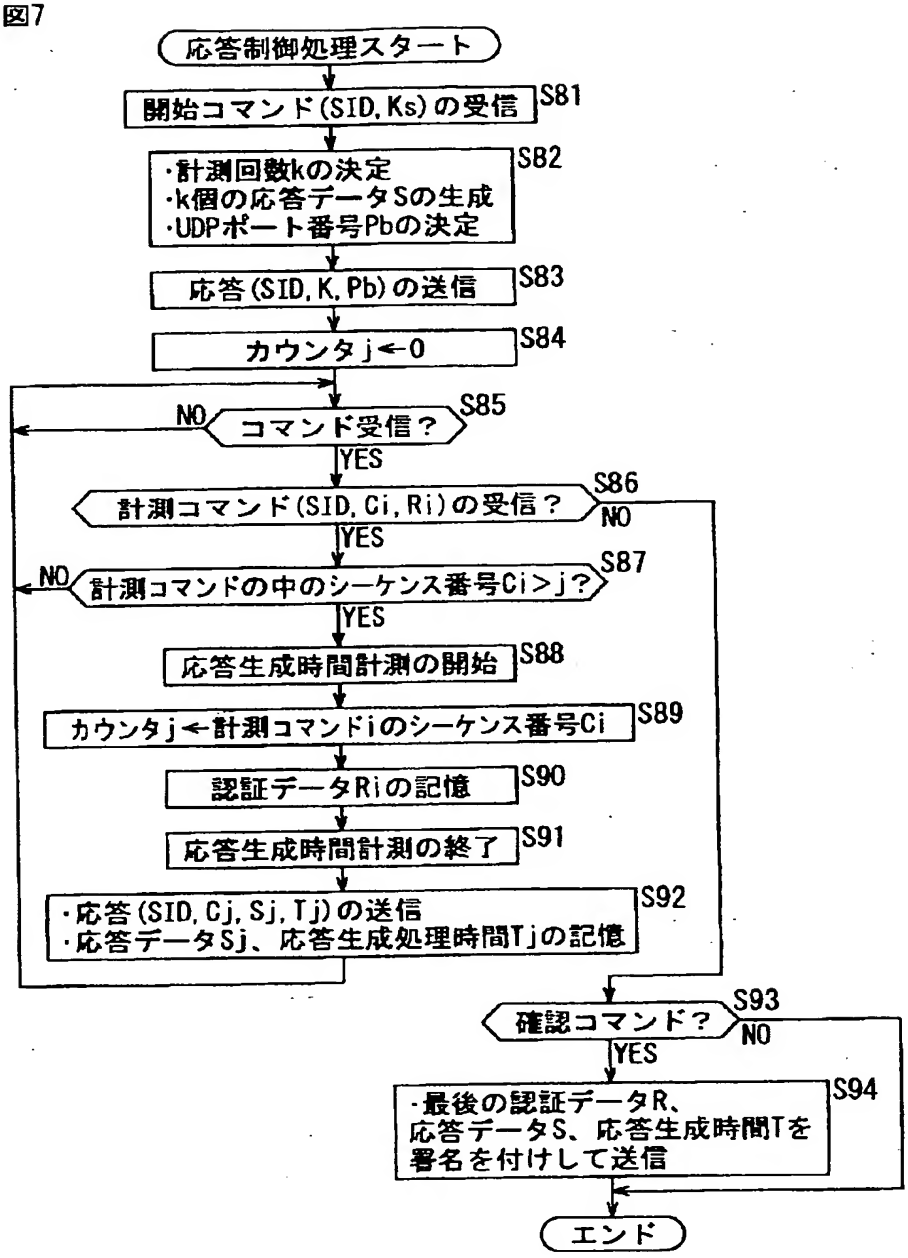
【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００７１
【補正方法】変更
【補正の内容】
【００７１】
ステップＳ５７で、まだ所定の時間が経過していないと判定された場合、ステップＳ５６に戻り、それ以降の処理が実行される。一方ステップＳ５７で所定の時間経過したと判定された場合、ステップＳ６２に進み、カウンタiの値がリトライ数kより大きいか否かが判定され（RTT計測がk回行われたか否かが判定され）、まだ大きくないと判定された場合（k回行われていない場合）、ステップＳ６３に進み、カウンタiの値を１だけインクリメントされて、ステップＳ５５に戻る。

【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００９０
【補正方法】変更

【補正の内容】
【００９０】
そして制御判定部３８は、応答CCRに示されるハッシュ値と、ここでのハッシュ処理の結果得られたハッシュ値が一致するか否かを判定し、一致すると判定した場合、RTT計測相手と、正規の機器のみが知り得る情報（署名）の提供者とが一致すると判定し、コンテンツを受信側の機器に送信できると判定する。RTT計測相手と正規の機器のみが知り得る情報の提供者とが一致することを確認するための認証データR、応答データS、および応答生成時間Tを、適宜、確認データQと称する。
【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】０１０９
【補正方法】変更
【補正の内容】
【０１０９】
ステップＳ９１において、計測コマンド受信部５３は、認証データRiの読み出しが完了した旨の通知ENDを応答生成時間計測部５４に行う。これにより応答生成時間計測部５４は、ステップＳ８８で開始した応答生成時間計測を終了し、計測結果Ｔｊを計測応答送信部５５および記憶部５６に供給する。
【手続補正１０】
【補正対象書類名】図面
【補正対象項目名】図７
【補正方法】変更
【補正の内容】

【図７】

図7


応答制御処理スタート
開始コマンド(SID, Ks)の受信
S81
・計測回数kの決定
・k個の応答データSの生成
・UDPポート番号Pbの決定
S82
応答(SID, K, Pb)の送信
S83
カウンタj←0
S84
NO
コマンド受信？
S85
YES
計測コマンド(SID, Ci, Ri)の受信？
S86
NO
YES
NO
計測コマンドの中のシーケンス番号Ci>j?
S87
YES
応答生成時間計測の開始
S88
カウンタj←計測コマンドiのシーケンス番号Ci
S89
認証データRiの記憶
S90
応答生成時間計測の終了
S91
・応答(SID, Cj, Sj, Tj)の送信
・応答データSj、応答生成処理時間Tjの記憶
S92
確認コマンド？
S93
NO
YES
・最後の認証データR、
応答データS、応答生成時間Tを
署名を付けして送信
S94
エンド